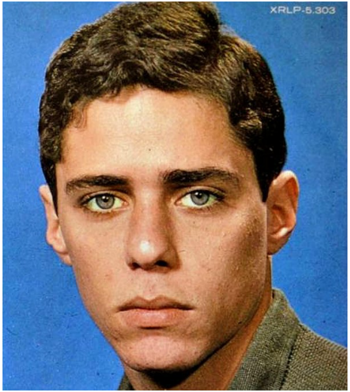
Quantum cryptography from weaker computational assumptions

Alex Bredariol Grilo

Quantum information vs. cryptography

Quantum information vs. cryptography



Quantum helps malicious parties

Quantum information vs. cryptography

Quantum helps honest parties   Quantum helps malicious parties

Quantum information vs. cryptography

Quantum helps honest parties Quantum helps malicious parties

How do quantum resources allow us to achieve better cryptographic protocols?

Quantum 101 (simplified)

Quantum mechanics

Quantum states	Evolution	Measurements

Quantum 101 (simplified)

Quantum mechanics

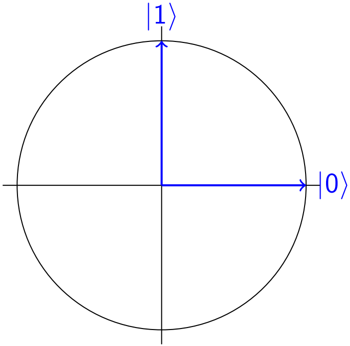
Quantum states	Evolution	Measurements

Quantum 101 (simplified)

Quantum mechanics

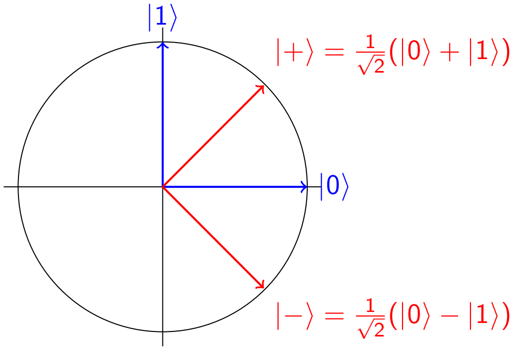
Quantum states | Evolution | Measurements

States



Quantum 101 (simplified)

States



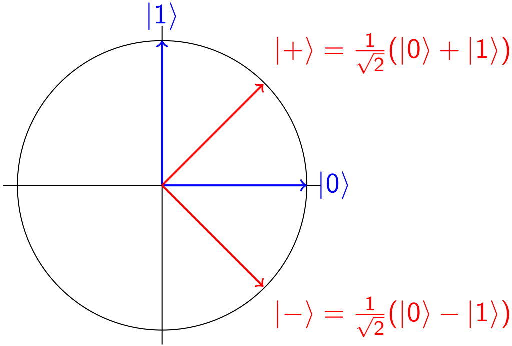
Measurements

Quantum 101 (simplified)

Quantum mechanics

Quantum states   Evolution   Measurements

States



Measurements

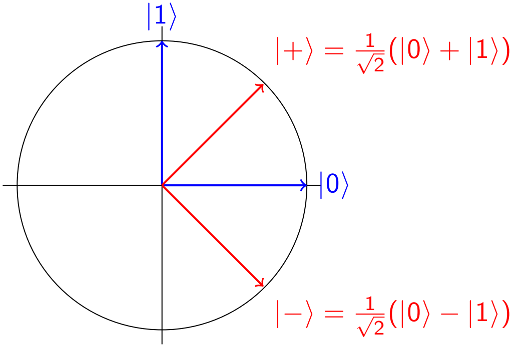
- Computational basis $\rightarrow$

Quantum 101 (simplified)

Quantum mechanics

Quantum states   Evolution   Measurements

States



Measurements

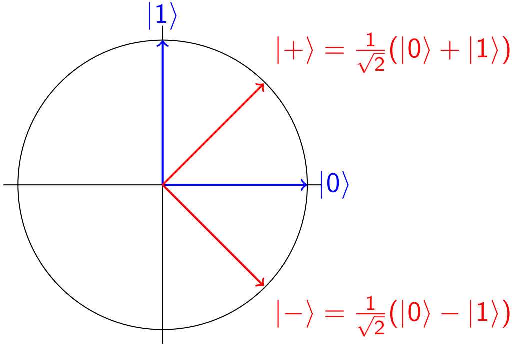
- Computational basis $\rightarrow$
  - Meas. $|0\rangle$, the outcome is 0 w.p. 1
  - Meas. $|1\rangle$, the outcome is 1 w.p. 1

Quantum 101 (simplified)

Quantum mechanics

Quantum states | Evolution | Measurements

States

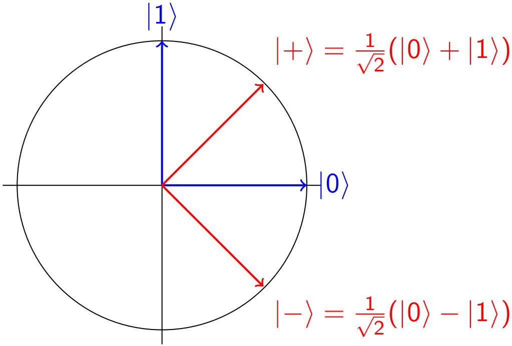


Measurements

- Computational basis $\rightarrow$
  - Meas. $|0\rangle$, the outcome is 0 w.p. 1
  - Meas. $|1\rangle$, the outcome is 1 w.p. 1
  - Meas. $|+\rangle$, the outcome is $0/1$ w.p. $1/2$
  - Meas. $|-\rangle$, the outcome is $0/1$ w.p. $1/2$

Quantum 101 (simplified)

States



Measurements

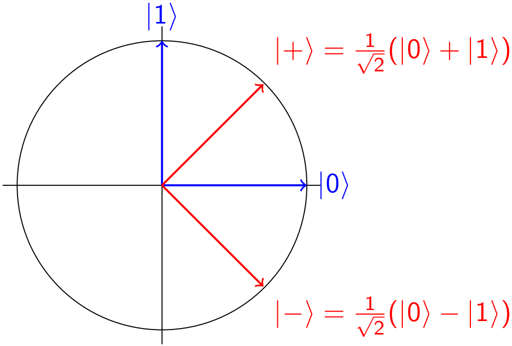
- Computational basis $\rightarrow$
  - Meas. $|0\rangle$, the outcome is 0 w.p. 1
  - Meas. $|1\rangle$, the outcome is 1 w.p. 1
  - Meas. $|+\rangle$, the outcome is $0/1$ w.p. $1/2$
  - Meas. $|-\rangle$, the outcome is $0/1$ w.p. $1/2$
- Hadamard basis $\nearrow$

Quantum 101 (simplified)

Quantum mechanics

Quantum states | Evolution | Measurements

States



Measurements

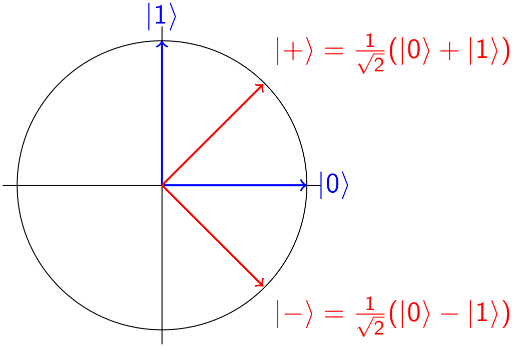
- Computational basis $\rightarrow$
  - Meas. $|0\rangle$, the outcome is 0 w.p. 1
  - Meas. $|1\rangle$, the outcome is 1 w.p. 1
  - Meas. $|+\rangle$, the outcome is $0/1$ w.p. $1/2$
  - Meas. $|-\rangle$, the outcome is $0/1$ w.p. $1/2$
- Hadamard basis $\nearrow$
  - Meas. $|0\rangle$, the outcome is $+/-$ w.p. $1/2$
  - Meas. $|1\rangle$, the outcome is $+/-$ w.p. $1/2$

Quantum 101 (simplified)

Quantum mechanics

Quantum states | Evolution | Measurements

States

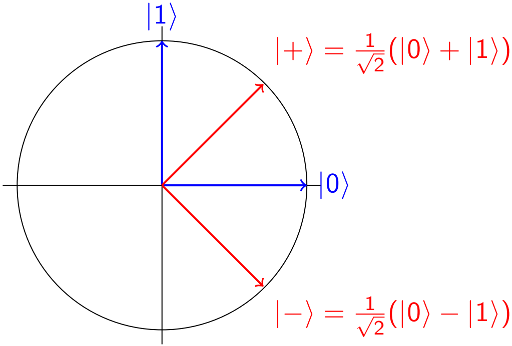


Measurements

- Computational basis $\rightarrow$
  - Meas. $|0\rangle$, the outcome is 0 w.p. 1
  - Meas. $|1\rangle$, the outcome is 1 w.p. 1
  - Meas. $|+\rangle$, the outcome is $0/1$ w.p. $1/2$
  - Meas. $|-\rangle$, the outcome is $0/1$ w.p. $1/2$
- Hadamard basis $\nearrow$
  - Meas. $|0\rangle$, the outcome is $+/-$ w.p. $1/2$
  - Meas. $|1\rangle$, the outcome is $+/-$ w.p. $1/2$
  - Meas. $|+\rangle$, the outcome is $+$ w.p. 1
  - Meas. $|-\rangle$, the outcome is $-$ w.p. 1

Quantum 101 (simplified)

States



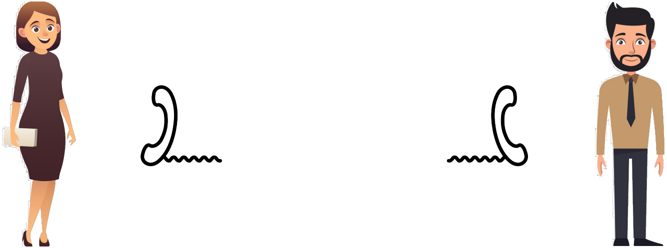
Measurements

- Computational basis $\rightarrow$
  - Meas. $|0\rangle$, the outcome is 0 w.p. 1
  - Meas. $|1\rangle$, the outcome is 1 w.p. 1
  - Meas. $|+\rangle$, the outcome is $0/1$ w.p. $1/2$
  - Meas. $|-\rangle$, the outcome is $0/1$ w.p. $1/2$
- Hadamard basis $\nearrow$
  - Meas. $|0\rangle$, the outcome is $+/-$ w.p. $1/2$
  - Meas. $|1\rangle$, the outcome is $+/-$ w.p. $1/2$
  - Meas. $|+\rangle$, the outcome is $+$ w.p. 1
  - Meas. $|-\rangle$, the outcome is $-$ w.p. 1

State collapses after measurements

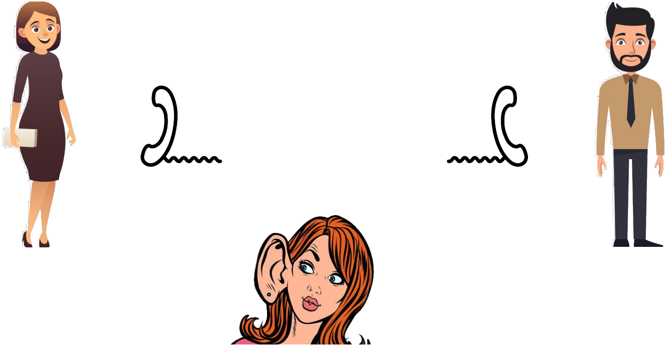
Key agreement

Key agreement



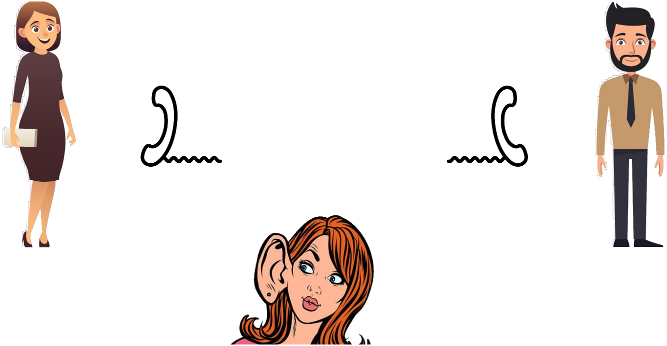
Goal: Alice and Bob want to share a common random key k by the phone

Key agreement



Goal: Alice and Bob want to share a common random key k by the phone
Security: They want k to be unknown to potential eavesdroppers

Key agreement



Goal: Alice and Bob want to share a common random key k by the phone
Security: They want k to be unknown to potential eavesdroppers
Classical information-theoretically secure key agreement is impossible!

Quantum-key distribution (simplified)

Quantum-key distribution (simplified)

Quantum-key distribution (simplified)

	Basis
$\lvert\phi_1\rangle = \lvert+\rangle$	1
$\lvert\phi_2\rangle = \lvert 0\rangle$	0
$\lvert\phi_3\rangle = \lvert 1\rangle$	0
$\lvert\phi_4\rangle = \lvert 0\rangle$	0
$\lvert\phi_5\rangle = \lvert-\rangle$	1
$\lvert\phi_6\rangle = \lvert-\rangle$	1

Quantum-key distribution (simplified)

	Basis
$\|\phi_1\rangle = \|+\rangle$	1
$\|\phi_2\rangle = \|0\rangle$	0
$\|\phi_3\rangle = \|1\rangle$	0
$\|\phi_4\rangle = \|0\rangle$	0
$\|\phi_5\rangle = \|-\rangle$	1
$\|\phi_6\rangle = \|-\rangle$	1

$$\xrightarrow{|{+}010{-}{-}\rangle}$$

Quantum-key distribution (simplified)

	Basis
$\lvert\phi_1\rangle = \lvert+\rangle$	1
$\lvert\phi_2\rangle = \lvert0\rangle$	0
$\lvert\phi_3\rangle = \lvert1\rangle$	0
$\lvert\phi_4\rangle = \lvert0\rangle$	0
$\lvert\phi_5\rangle = \lvert-\rangle$	1
$\lvert\phi_6\rangle = \lvert-\rangle$	1

$$\xrightarrow{\lvert+010--\rangle}$$

Basis	Outcome
1	$+$
1	$-$
0	1
0	0
0	0
1	$-$

Quantum-key distribution (simplified)

	Basis
$\vert\phi_1\rangle = \vert+\rangle$	1
$\vert\phi_2\rangle = \vert 0\rangle$	0
$\vert\phi_3\rangle = \vert 1\rangle$	0
$\vert\phi_4\rangle = \vert 0\rangle$	0
$\vert\phi_5\rangle = \vert-\rangle$	1
$\vert\phi_6\rangle = \vert-\rangle$	1

$$\xrightarrow{\quad |+010--\rangle \quad}$$

$$\xleftarrow{\quad 110001 \quad}$$

Basis	Outcome
1	$+$
1	$-$
0	1
0	0
0	0
1	$-$

Quantum-key distribution (simplified)

	Basis
$\lvert\phi_1\rangle = \lvert+\rangle$	1
$\lvert\phi_2\rangle = \lvert 0\rangle$	0
$\lvert\phi_3\rangle = \lvert 1\rangle$	0
$\lvert\phi_4\rangle = \lvert 0\rangle$	0
$\lvert\phi_5\rangle = \lvert-\rangle$	1
$\lvert\phi_6\rangle = \lvert-\rangle$	1

$\xrightarrow{\lvert +010--\rangle}$

$\xleftarrow{110001}$

$\xrightarrow{100011,\ \mathrm{T} = \{1,4\}}$

Basis	Outcome
1	$+$
1	$-$
0	1
0	0
0	0
1	$-$

Quantum-key distribution (simplified)

	Basis
$\color{blue}{\lvert\phi_1\rangle = \lvert+\rangle}$	$\color{blue}{1}$
$\lvert\phi_2\rangle = \lvert 0\rangle$	0
$\color{blue}{\lvert\phi_3\rangle = \lvert 1\rangle}$	$\color{blue}{0}$
$\color{blue}{\lvert\phi_4\rangle = \lvert 0\rangle}$	$\color{blue}{0}$
$\lvert\phi_5\rangle = \lvert -\rangle$	1
$\color{blue}{\lvert\phi_6\rangle = \lvert -\rangle}$	$\color{blue}{1}$

$$\xrightarrow{\quad\lvert+010--\rangle\quad}$$

$$\xleftarrow{\quad 110001\quad}$$

$$\xrightarrow{\quad 100011,\ \mathrm{T} = \{1,4\}\quad}$$

$$\xleftarrow{\quad +0\quad}$$

Basis	Outcome
$\color{blue}{1}$	$\color{blue}{+}$
1	$-$
$\color{blue}{0}$	$\color{blue}{1}$
$\color{blue}{0}$	$\color{blue}{0}$
0	0
$\color{blue}{1}$	$\color{blue}{-}$

Quantum-key distribution (simplified)

	Basis
$\|\phi_1\rangle = \|+\rangle$	1
$\|\phi_2\rangle = \|0\rangle$	0
$\|\phi_3\rangle = \|1\rangle$	0
$\|\phi_4\rangle = \|0\rangle$	0
$\|\phi_5\rangle = \|-\rangle$	1
$\|\phi_6\rangle = \|-\rangle$	1

$$\xrightarrow{\;|{+}010--\rangle\;}$$

$$\xleftarrow{\;110001\;}$$

$$\xrightarrow{\;100011,\ \mathrm{T} = \{1{,}4\}\;}$$

$$\xleftarrow{\;+0\;}$$

Basis	Outcome
1	$+$
1	$-$
0	1
0	0
0	0
1	$-$

Quantum-key distribution (simplified)

	Basis
$\vert\phi_1\rangle = \vert+\rangle$	1
$\vert\phi_2\rangle = \vert 0\rangle$	0
$\vert\phi_3\rangle = \vert 1\rangle$	0
$\vert\phi_4\rangle = \vert 0\rangle$	0
$\vert\phi_5\rangle = \vert-\rangle$	1
$\vert\phi_6\rangle = \vert-\rangle$	1

$\xrightarrow{\;|{+}010{-}{-}\rangle\;}$

$\xleftarrow{\;110001\;}$

$\xrightarrow{\;100011,\ \mathsf{T} = \{1{,}4\}\;}$

$\xleftarrow{\;+0\;}$

Basis	Outcome
1	+
1	−
0	1
0	0
0	0
1	−

- Intuitively, if Eve tries to eavesdrop the quantum state, it collapses

Quantum-key distribution (simplified)

	Basis
$\lvert\phi_1\rangle = \lvert+\rangle$	1
$\lvert\phi_2\rangle = \lvert0\rangle$	0
$\lvert\phi_3\rangle = \lvert1\rangle$	0
$\lvert\phi_4\rangle = \lvert0\rangle$	0
$\lvert\phi_5\rangle = \lvert-\rangle$	1
$\lvert\phi_6\rangle = \lvert-\rangle$	1

$$\xrightarrow{\lvert+010--\rangle}$$

$$\xleftarrow{110001}$$

$$\xrightarrow{100011,\ \mathsf{T} = \{1,4\}}$$

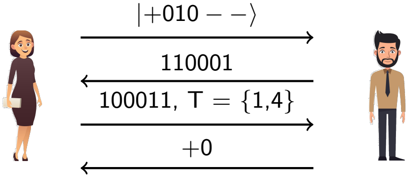
$$\xleftarrow{+0}$$

Basis	Outcome
1	$+$
1	$-$
0	1
0	0
0	0
1	$-$

- Intuitively, if Eve tries to eavesdrop the quantum state, it collapses
  - Complete protocol and formal security proof is more cumbersome

Quantum-key distribution (simplified)

	Basis
$\vert\phi_1\rangle = \vert+\rangle$	1
$\vert\phi_2\rangle = \vert0\rangle$	0
$\vert\phi_3\rangle = \vert1\rangle$	0
$\vert\phi_4\rangle = \vert0\rangle$	0
$\vert\phi_5\rangle = \vert-\rangle$	1
$\vert\phi_6\rangle = \vert-\rangle$	1



Basis	Outcome
1	$+$
1	$-$
0	1
0	0
0	0
1	$-$

- Intuitively, if Eve tries to eavesdrop the quantum state, it collapses
  - Complete protocol and formal security proof is more cumbersome
- Can we achieve other protocols such as bit-commitment, MPC,... unconditionally?

Quantum-key distribution (simplified)

	Basis
$\lvert\phi_1\rangle = \lvert+\rangle$	1
$\lvert\phi_2\rangle = \lvert 0\rangle$	0
$\lvert\phi_3\rangle = \lvert 1\rangle$	0
$\lvert\phi_4\rangle = \lvert 0\rangle$	0
$\lvert\phi_5\rangle = \lvert-\rangle$	1
$\lvert\phi_6\rangle = \lvert-\rangle$	1

$\xrightarrow{\lvert +010--\rangle}$

$\xleftarrow{110001}$

$\xrightarrow{100011,\ T=\{1,4\}}$

$\xleftarrow{+0}$

Basis	Outcome
1	$+$
1	$-$
0	1
0	0
0	0
1	$-$

- Intuitively, if Eve tries to eavesdrop the quantum state, it collapses
  - Complete protocol and formal security proof is more cumbersome
- Can we achieve other protocols such as bit-commitment, MPC,... unconditionally?
- No! [M'97, LC'97]

Quantum-key distribution (simplified)

	Basis
$\vert\phi_1\rangle = \vert+\rangle$	1
$\vert\phi_2\rangle = \vert 0\rangle$	0
$\vert\phi_3\rangle = \vert 1\rangle$	0
$\vert\phi_4\rangle = \vert 0\rangle$	0
$\vert\phi_5\rangle = \vert-\rangle$	1
$\vert\phi_6\rangle = \vert-\rangle$	1

$\xrightarrow{\vert+010--\rangle}$

$\xleftarrow{110001}$

$\xrightarrow{100011,\ \mathsf{T} = \{1,4\}}$

$\xleftarrow{+0}$

Basis	Outcome
1	$+$
1	$-$
0	1
0	0
0	0
1	$-$

- Intuitively, if Eve tries to eavesdrop the quantum state, it collapses
  - Complete protocol and formal security proof is more cumbersome
- Can we achieve other protocols such as bit-commitment, MPC,... unconditionally?
- No! [M'97, LC'97]

What if we use computational assumptions?

Classical cryptographic primitive/assumptions

Public-key encryption

Functional encryption

Oblivious transfer

indistinguishable Obfuscation

Secret-key encryption

Two-party computation

Witness encryption

Multi-party computation

One-way functions

Pseudo-random number generators

Zero-knowledge proof systems

How to propose implementations and prove their security?

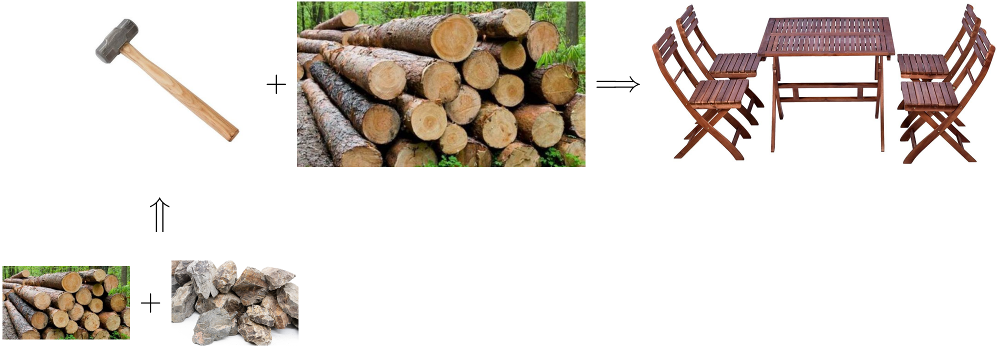
Reductions

Reductions

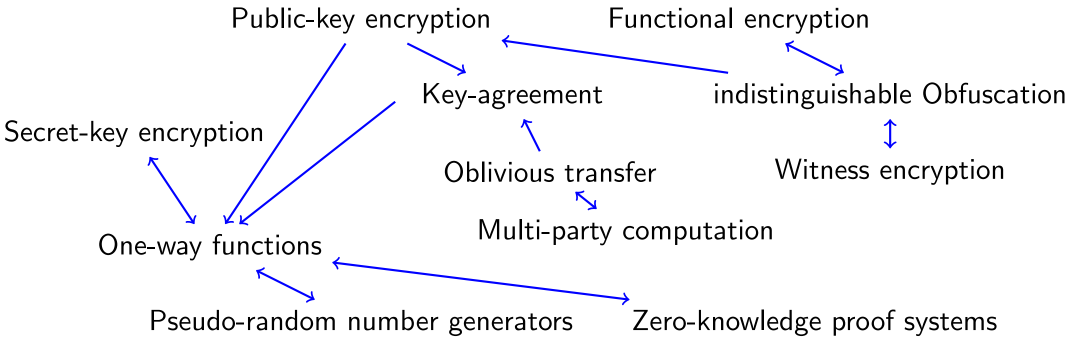
$+$

$\Longrightarrow$

Reductions

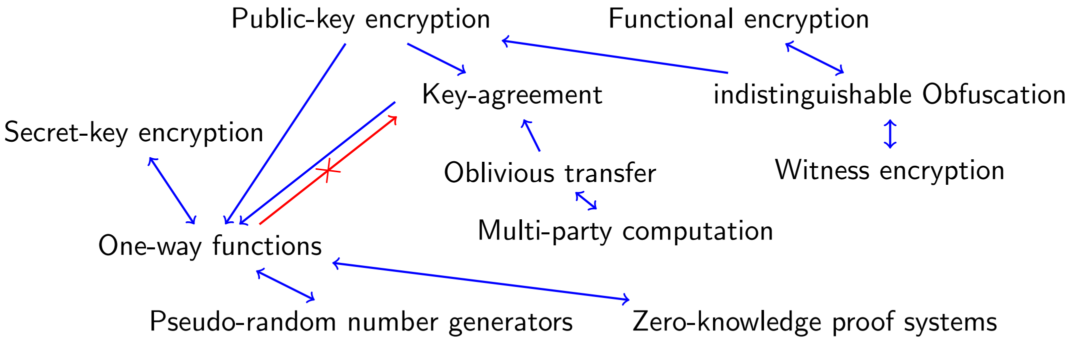


Primitives

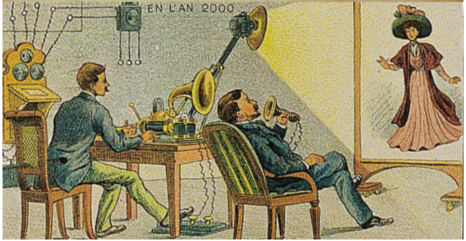


Public-key encryption
Functional encryption
Key-agreement
indistinguishable Obfuscation
Secret-key encryption
Oblivious transfer
Witness encryption
Multi-party computation
One-way functions
Pseudo-random number generators
Zero-knowledge proof systems

Primitives

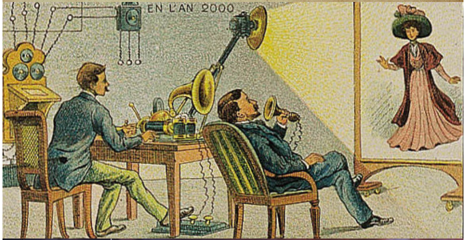

Public-key encryption
Functional encryption
Key-agreement
indistinguishable Obfuscation
Secret-key encryption
Oblivious transfer
Witness encryption
Multi-party computation
One-way functions
Pseudo-random number generators
Zero-knowledge proof systems

Minicrypt: OWFs exist



Cryptomania: PKE schemes exist

Minicrypt: OWFs exist



Cryptomania: PKE schemes exist

Obfutopia: iO exists

… if crypto is possible

Algorithmica(+Heuristica): We can solve NP (in practice)

Pessiland: We cannot solve NP and OWFs do not exist

Minicrypt

Minicrypt

One-way function f

For every polynomial-time adversary $\mathcal{A}$, and polynomial ℓ:

$$\Pr_x[\mathcal{A}(f(x)) \in f^{-1}(x)] \leq negl(n).$$

Minicrypt

One-way function f

For every polynomial-time adversary $\mathcal{A}$, and polynomial ℓ:

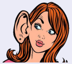
$$\Pr_x[\mathcal{A}(f(x)) \in f^{-1}(x)] \leq negl(n).$$

Symmetric-key encryption

sk

$c = Enc_{sk}(m)$

$\longleftarrow$



sk

$m' = Dec_{sk}(c)$

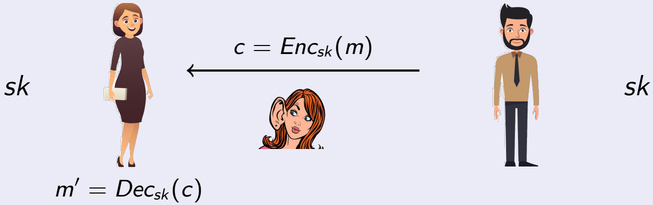
Minicrypt

One-way function f

For every polynomial-time adversary $\mathcal{A}$, and polynomial ℓ:

$$\Pr_x[\mathcal{A}(f(x)) \in f^{-1}(x)] \le negl(n).$$

Symmetric-key encryption



Pseudo-random function $\{f_k\}_k$

For every polynomial-time adversary $\mathcal{A}$:

$$|\Pr_k[\mathcal{A}^{f_k}() = 1] - \Pr_{f \sim U}[\mathcal{A}^f() = 1]| \le negl(n).$$

This talk

1. Quantum protocols for public-key encryption
2. Quantum protocols for multi-party computation
3. Weaker assumptions in the quantum world

Quantum protocols for public-key encryption

Public-key encryption

Public-key encryption

$$Gen(1^n) = (sk, pk)$$

sk

Public-key encryption

pk

sk

Public-key encryption

pk

sk

$c = Enc_{pk}(m)$

Public-key encryption

pk

sk

$c = Enc_{pk}(m)$

$m' = Dec_{sk}(c)$

Public-key encryption

pk

sk

$c = Enc_{pk}(m)$

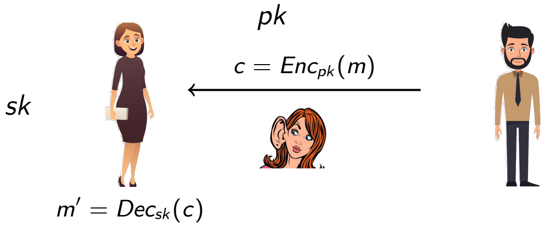
$\longleftarrow$

$m' = Dec_{sk}(c)$

Correctness

$$Dec_{sk}(Enc_{pk}(m)) = m$$

Public-key encryption



Correctness

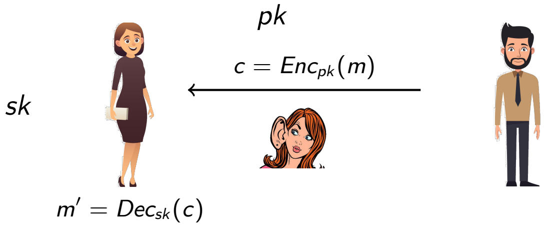
$$Dec_{sk}(Enc_{pk}(m)) = m$$

Security (simplified)

For every polynomial-time adversary $\mathcal{A}$:

$|\Pr[\mathcal{A}(pk, Enc_{pk}(0)) = 1] - \Pr[\mathcal{A}(pk, Enc_{pk}(1)) = 1]| \leq negl(n)$.

Public-key encryption



Correctness

$$Dec_{sk}(Enc_{pk}(m)) = m$$

Security (simplified)

For every polynomial-time adversary $\mathcal{A}$:

$|\Pr[\mathcal{A}(pk, Enc_{pk}(0)) = 1] - \Pr[\mathcal{A}(pk, Enc_{pk}(1)) = 1]| \leq negl(n)$.

Theorem [IR'89]

PKE cannot be built from OWF in a black-box way

Public-key encryption with quantum public keys

Public-key encryption with quantum public keys

$$Gen(1^n) = (sk, |pk\rangle^{\otimes \ell})$$

sk

Public-key encryption with quantum public keys

$|pk\rangle^{\otimes \ell}$

sk

Public-key encryption with quantum public keys

$|pk\rangle^{\otimes \ell}$

sk

$c = Enc_{|pk\rangle}(m)$

Public-key encryption with quantum public keys

$|pk\rangle^{\otimes \ell}$

$c = Enc_{|pk\rangle}(m)$

sk

$\longleftarrow$

$m' = Dec_{sk}(c)$

Public-key encryption with quantum public keys

$|pk\rangle^{\otimes \ell}$

$c = Enc_{|pk\rangle}(m)$

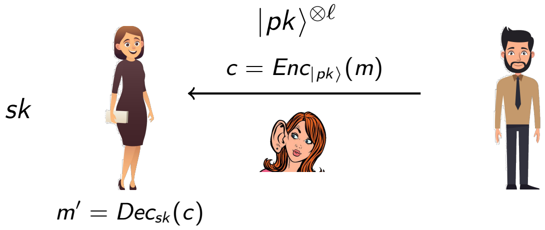
sk

$m' = Dec_{sk}(c)$

Correctness

$$Dec_{sk}(Enc_{|pk\rangle}(m)) = m$$

Public-key encryption with quantum public keys



Correctness

$$Dec_{sk}(Enc_{|pk\rangle}(m)) = m$$

Security (simplified)

For every polynomial-time adversary $\mathcal{A}$, and polynomial ℓ:
$|\Pr[\mathcal{A}(|pk\rangle^{\otimes \ell}, Enc_{|pk\rangle}(0)) = 1] - \Pr[\mathcal{A}(|pk\rangle^{\otimes \ell}, Enc_{|pk\rangle}(1)) = 1]| \leq negl(n)$.

QPKE from OWF [BGHMSVW'23]

QPKE from OWF [BGHMSVW'23]

Construction

QPKE from OWF [BGHMSVW'23]

Construction

- $sk = k$ and $|pk\rangle = \frac{1}{\sqrt{2^n}} \sum_x |x\rangle |PRF_k(x)\rangle$

QPKE from OWF [BGHMSVW'23]

Construction

- $sk = k$ and $|pk\rangle = \frac{1}{\sqrt{2^n}} \sum_x |x\rangle |PRF_k(x)\rangle$
- $Enc_{|pk\rangle}(m)$:
  1. Measure $|pk\rangle$ and get $(x^*, PRF_k(x^*))$
  2. $c = (x^*, c^* = SE.Enc_{PRF_k(x^*)}(m))$

QPKE from OWF [BGHMSVW'23]

Construction

- $sk = k$ and $|pk\rangle = \frac{1}{\sqrt{2^n}} \sum_x |x\rangle|PRF_k(x)\rangle$
- $Enc_{|pk\rangle}(m)$:
  1. Measure $|pk\rangle$ and get $(x^*, PRF_k(x^*))$
  2. $c = (x^*, c^* = SE.Enc_{PRF_k(x^*)}(m))$
- $Dec_k((x^*, c^*)) = SE.Dec_{PRF_k(x^*)}(c^*)$

QPKE from OWF [BGHMSVW'23]

Construction

- $sk = k$ and $|pk\rangle = \frac{1}{\sqrt{2^n}} \sum_x |x\rangle |PRF_k(x)\rangle$
- $Enc_{|pk\rangle}(m)$:
  1. Measure $|pk\rangle$ and get $(x^*, PRF_k(x^*))$
  2. $c = (x^*, c^* = SE.Enc_{PRF_k(x^*)}(m))$
- $Dec_k((x^*, c^*)) = SE.Dec_{PRF_k(x^*)}(c^*)$

- Correctness follows from correctness of PRF and SKE

QPKE from OWF [BGHMSVW'23]

Construction

- $sk = k$ and $|pk\rangle = \frac{1}{\sqrt{2^n}} \sum_x |x\rangle|PRF_k(x)\rangle$
- $Enc_{|pk\rangle}(m)$:
  1. Measure $|pk\rangle$ and get $(x^*, PRF_k(x^*))$
  2. $c = (x^*, c^* = SE.Enc_{PRF_k(x^*)}(m))$
- $Dec_k((x^*, c^*)) = SE.Dec_{PRF_k(x^*)}(c^*)$

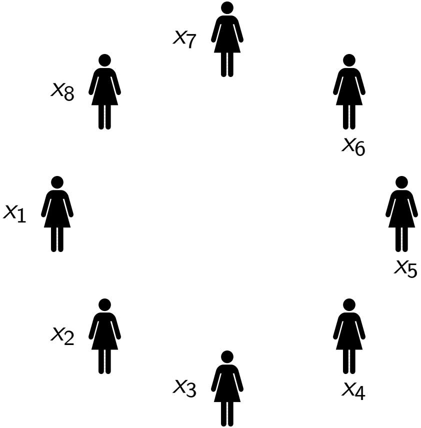
- Correctness follows from correctness of PRF and SKE
- Security comes from SKE, PRF and randomness of quantum measurements

Further results

- Impossibility of information-theoretically secure QPKE [B**G**HMSVW'23]
- QPKE from pseudo-random states (with special properties) [B**G**HMSVW'23]
- Quantum trapdoor functions and quantum PKE [C'23]
- Tamper-resilient QPKE from OWF [KMNY'23]
- Non-interactive KE from OWF [MW'23]

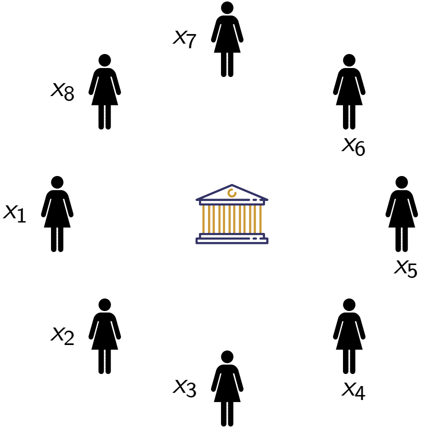
Quantum protocols for multi-party computation

Multi-party computation



Goal: Compute $f(x_1, ..., x_8)$ without revealing their input

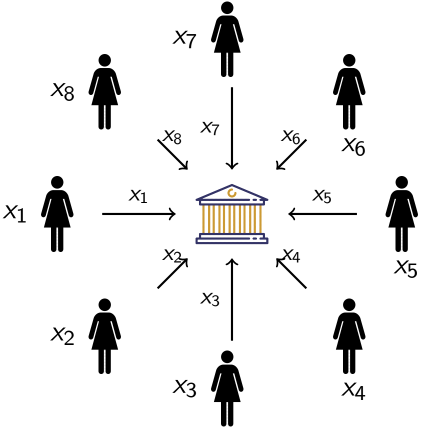
Multi-party computation



Goal: Compute $f(x_1, \ldots, x_8)$ without revealing their input

Ideal world

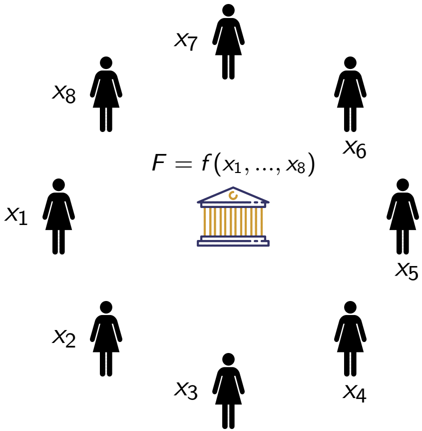
Multi-party computation



Goal: Compute $f(x_1, \ldots, x_8)$ without revealing their input

Ideal world

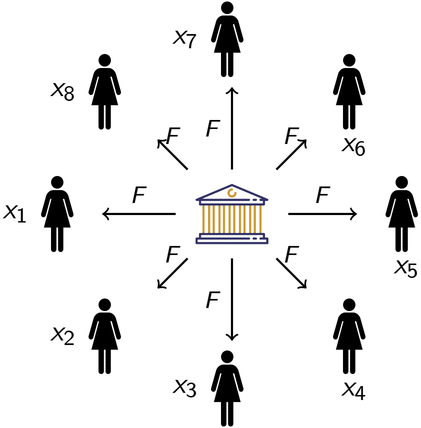
Multi-party computation



Goal: Compute $f(x_1, ..., x_8)$ without revealing their input

Ideal world

Multi-party computation

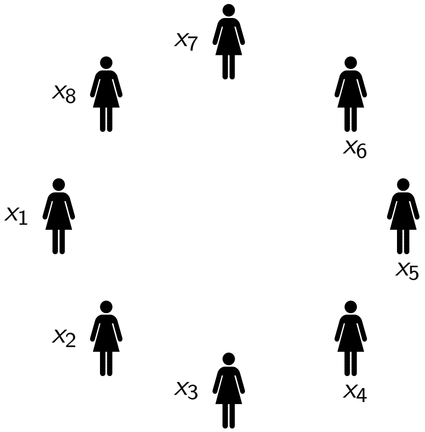


Goal: Compute $f(x_1, ..., x_8)$ without revealing their input

Ideal world

- Each party learns $F = f(x_1, ..., x_8)$ and nothing else

Multi-party computation



Goal: Compute $f(x_1, ..., x_8)$ without revealing their input

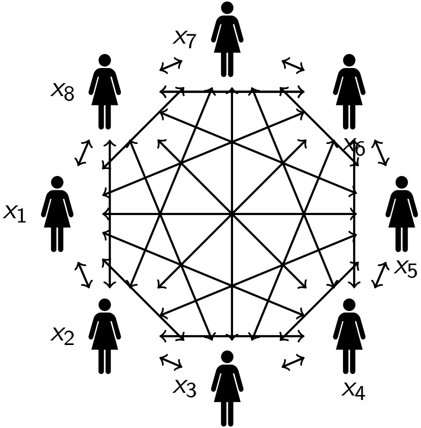
Ideal world

- Each party learns $F = f(x_1, ..., x_8)$ and nothing else

Real world

- Goal: implement the ideal functionality

Multi-party computation



Goal: Compute $f(x_1, \ldots, x_8)$ without revealing their input

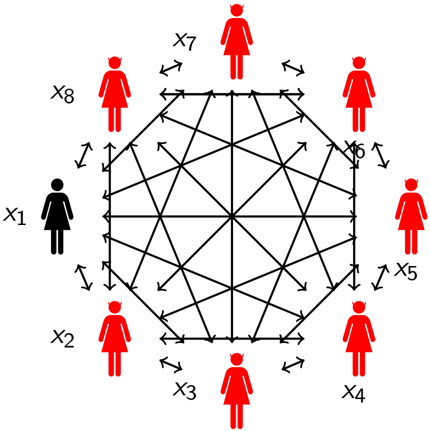
Ideal world

- Each party learns $F = f(x_1, \ldots, x_8)$ and nothing else

Real world

- Goal: implement the ideal functionality
- Protocols where parties interact, but still they only learn F

Multi-party computation



Goal: Compute $f(x_1, ..., x_8)$ without revealing their input

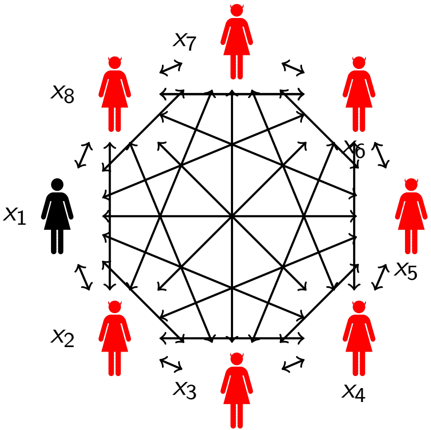
Ideal world

- Each party learns $F = f(x_1, ..., x_8)$ and nothing else

Real world

- Goal: implement the ideal functionality
- Protocols where parties interact, but still they only learn F
- Even if they behave disonestly

Multi-party computation



Goal: Compute $f(x_1, ..., x_8)$ without revealing their input

Ideal world

- Each party learns $F = f(x_1, ..., x_8)$ and nothing else

Real world

- Goal: implement the ideal functionality
- Protocols where parties interact, but still they only learn F
- Even if they behave disonestly

Theorem [MMP'12]

MPC cannot be built from OWF in a black-box way

Oblivious transfer

Oblivious transfer

Ideal functionality

S $\qquad$ $\mathcal{F}_{\texttt{ot}}$ $\qquad$ R

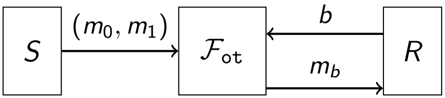
Oblivious transfer

Ideal functionality

$$\begin{tikzcd} \boxed{S} \arrow[r, "(m_0, m_1)"] & \boxed{\mathcal{F}_{\texttt{ot}}} & \boxed{R} \arrow[l, "b"'] \end{tikzcd}$$

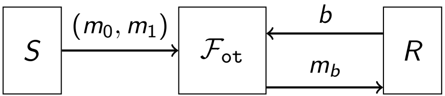
Oblivious transfer

Ideal functionality

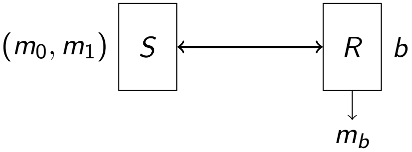


Oblivious transfer

Ideal functionality



Real world



MPC from Quantum+OWF

- IPS'08: MPC protocols from $\mathcal{F}_{ot}$

MPC from Quantum+OWF

- IPS'08: MPC protocols from $\mathcal{F}_{ot}$
- U'10: Classical reduction from $\mathcal{F}_{ot}$ to MPC holds in the quantum world

MPC from Quantum+OWF

- IPS'08: MPC protocols from $\mathcal{F}_{ot}$
- U'10: Classical reduction from $\mathcal{F}_{ot}$ to MPC holds in the quantum world
- CK'88/BBCS'92: Quantum protocol for OT based on commitment schemes

MPC from Quantum+OWF

- IPS'08: MPC protocols from $\mathcal{F}_{ot}$
- U'10: Classical reduction from $\mathcal{F}_{ot}$ to MPC holds in the quantum world
- CK'88/BBCS'92: Quantum protocol for OT based on commitment schemes
- DFLSS'09 BF'10: Security proof of CK/BBCS protocol based on strong classical commitment schemes (likely to lie outside of MiniCrypt)

MPC from Quantum+OWF

- IPS'08: MPC protocols from $\mathcal{F}_{ot}$
- U'10: Classical reduction from $\mathcal{F}_{ot}$ to MPC holds in the quantum world
- CK'88/BBCS'92: Quantum protocol for OT based on commitment schemes
- DFLSS'09 BF'10: Security proof of CK/BBCS protocol based on strong classical commitment schemes (likely to lie outside of MiniCrypt)
- BCKM'21 and **G**LSV'21: Quantum protocol for strong commitment from OWF

MPC from Quantum+OWF

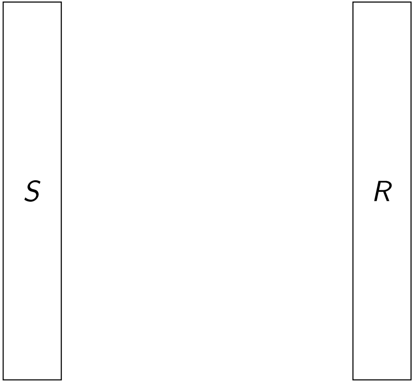
- IPS'08: MPC protocols from $\mathcal{F}_{ot}$
- U'10: Classical reduction from $\mathcal{F}_{ot}$ to MPC holds in the quantum world
- CK'88/BBCS'92: Quantum protocol for OT based on commitment schemes
- DFLSS'09 BF'10: Security proof of CK/BBCS protocol based on strong classical commitment schemes (likely to lie outside of MiniCrypt)
- BCKM'21 and **G**LSV'21: Quantum protocol for strong commitment from OWF

Corollary

Quantum protocol for MPC from OWF

CK/BBCS protocol (I)

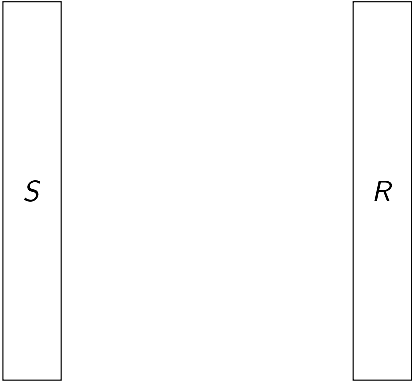
CK/BBCS protocol (I)



CK/BBCS protocol (I)

$\vec{x} \in \{0,1\}^\lambda$

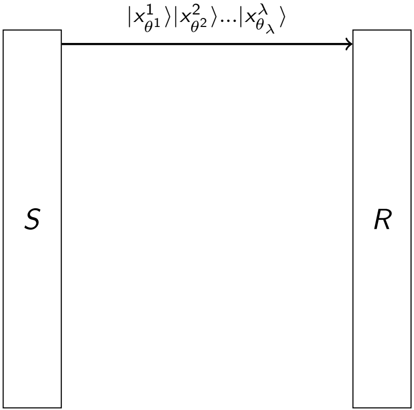
$\vec{\theta} \in \{+,\times\}^\lambda$



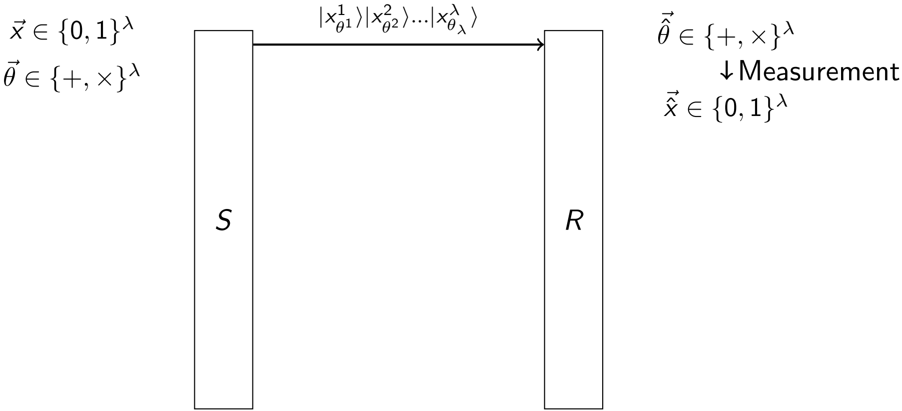
CK/BBCS protocol (I)

$\vec{x} \in \{0,1\}^\lambda$

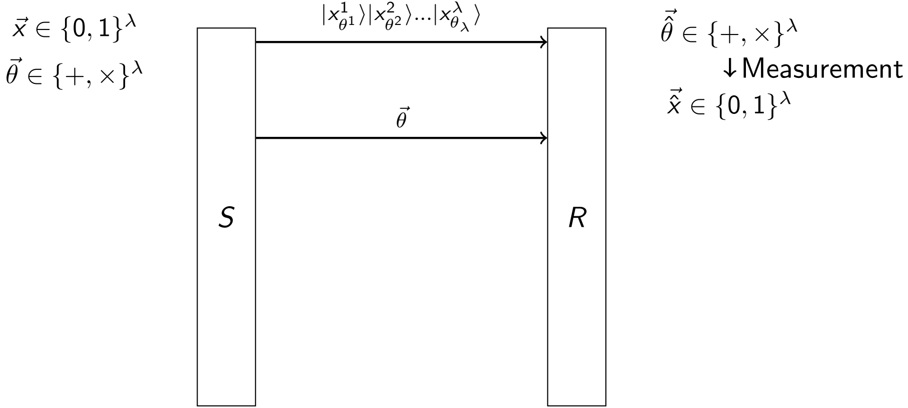
$\vec{\theta} \in \{+,\times\}^\lambda$



CK/BBCS protocol (I)



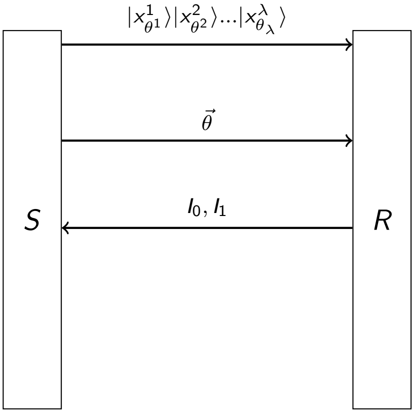
CK/BBCS protocol (I)



CK/BBCS protocol (I)

$\vec{x} \in \{0,1\}^\lambda$

$\vec{\theta} \in \{+,\times\}^\lambda$



$\vec{\hat{\theta}} \in \{+,\times\}^\lambda$

$\downarrow$ Measurement

$\vec{\hat{x}} \in \{0,1\}^\lambda$

$I_b = \{i : \theta_i = \hat{\theta}_i\}$

$I_{\overline{b}} = \{i : \theta_i \neq \hat{\theta}_i\}$

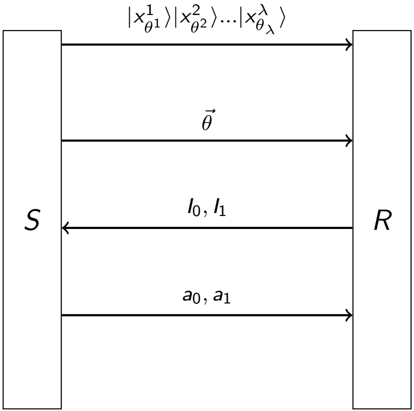
CK/BBCS protocol (I)

$\vec{x} \in \{0,1\}^\lambda$

$\vec{\theta} \in \{+,\times\}^\lambda$

$a_0 = Enc_{\vec{x}_{I_0}}(m_0)$

$a_1 = Enc_{\vec{x}_{I_1}}(m_0)$



$\vec{\hat{\theta}} \in \{+,\times\}^\lambda$

$\downarrow$ Measurement

$\vec{\hat{x}} \in \{0,1\}^\lambda$

$I_b = \{i : \theta_i = \hat{\theta}_i\}$

$I_{\overline{b}} = \{i : \theta_i \neq \hat{\theta}_i\}$

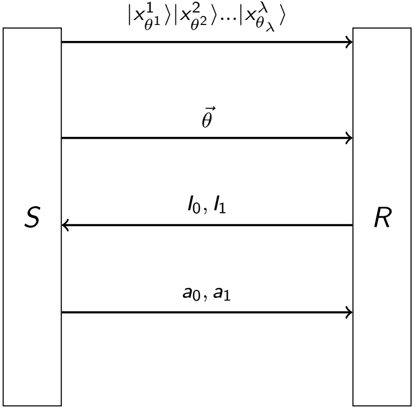
CK/BBCS protocol (I)

$\vec{x} \in \{0,1\}^\lambda$

$\vec{\theta} \in \{+,\times\}^\lambda$

$a_0 = Enc_{\vec{x}_{I_0}}(m_0)$

$a_1 = Enc_{\vec{x}_{I_1}}(m_0)$



$\vec{\hat{\theta}} \in \{+,\times\}^\lambda$

$\downarrow$ Measurement

$\vec{\hat{x}} \in \{0,1\}^\lambda$

$I_b = \{i : \theta_i = \hat{\theta}_i\}$

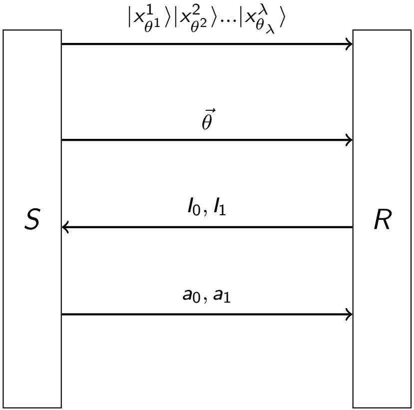
$I_{\overline{b}} = \{i : \theta_i \neq \hat{\theta}_i\}$

$m_b = Dec_{\vec{\hat{x}}_{I_b}}(a_b)$

CK/BBCS protocol (I)

$\vec{x} \in \{0,1\}^\lambda$

$\vec{\theta} \in \{+,\times\}^\lambda$



$\hat{\vec{\theta}} \in \{+,\times\}^\lambda$

$\downarrow$Measurement

$\hat{\vec{x}} \in \{0,1\}^\lambda$

$a_0 = Enc_{\vec{x}_{I_0}}(m_0)$

$a_1 = Enc_{\vec{x}_{I_1}}(m_0)$

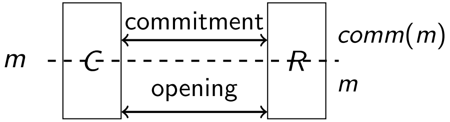
$I_b = \{i : \theta_i = \hat{\theta}_i\}$

$I_{\overline{b}} = \{i : \theta_i \neq \hat{\theta}_i\}$

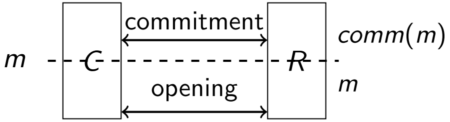
$m_b = Dec_{\hat{\vec{x}}_{I_b}}(a_b)$

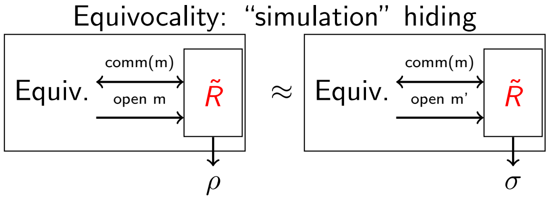
Attack for malicious receiver: $\tilde{R}$ waits $\vec{\theta}$ to measure the qubits using the right basis

Bit-commitment with simulation security

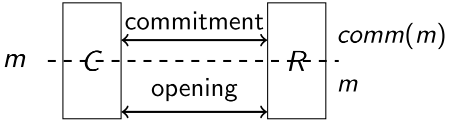


Bit-commitment with simulation security

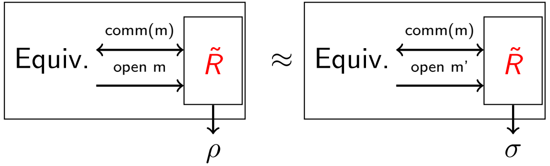




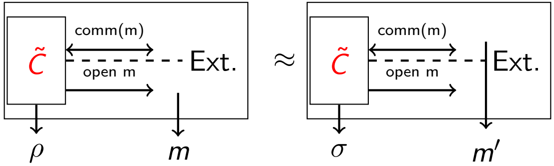
Bit-commitment with simulation security



Equivocality: "simulation" hiding



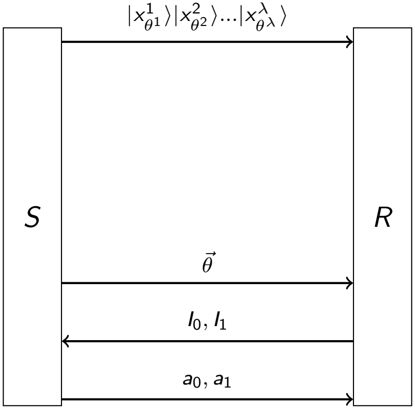
Extractability: "simulation" binding



CK/BBCS protocol (II)

$\vec{x} \in \{0,1\}^\lambda$

$\vec{\theta} \in \{+,\times\}^\lambda$



$\vec{\hat{\theta}} \in \{+,\times\}^\lambda$

$\downarrow$ Measurement

$\vec{\hat{x}} \in \{0,1\}^\lambda$

$I_b = \{i : \theta_i = \hat{\theta}_i\}$

$I_{\bar{b}} = \{i : \theta_i \neq \hat{\theta}_i\}$

$a_0 = Enc_{\vec{x}_{I_0}}(m_0)$

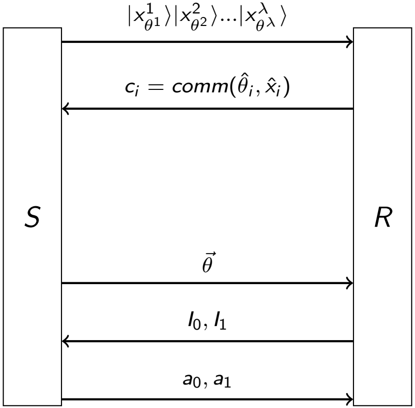
$a_1 = Enc_{\vec{x}_{I_1}}(m_0)$

$m_b = Dec_{\vec{\hat{x}}_{I_b}}(a_b)$

CK/BBCS protocol (II)

$\vec{x} \in \{0,1\}^\lambda$

$\vec{\theta} \in \{+,\times\}^\lambda$



$\vec{\hat{\theta}} \in \{+,\times\}^\lambda$

$\downarrow$Measurement

$\vec{\hat{x}} \in \{0,1\}^\lambda$

$a_0 = Enc_{\vec{x}_{I_0}}(m_0)$

$a_1 = Enc_{\vec{x}_{I_1}}(m_0)$

$I_b = \{i : \theta_i = \hat{\theta}_i\}$

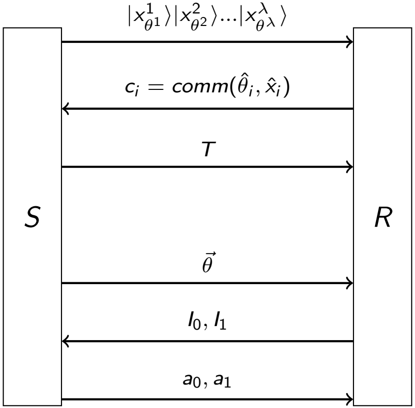
$I_{\bar{b}} = \{i : \theta_i \neq \hat{\theta}_i\}$

$m_b = Dec_{\vec{\hat{x}}_{I_b}}(a_b)$

CK/BBCS protocol (II)

$\vec{x} \in \{0,1\}^\lambda$

$\vec{\theta} \in \{+,\times\}^\lambda$



$\vec{\hat{\theta}} \in \{+,\times\}^\lambda$

↓Measurement

$\vec{\hat{x}} \in \{0,1\}^\lambda$

$I_b = \{i : \theta_i = \hat{\theta}_i\}$

$I_{\bar{b}} = \{i : \theta_i \neq \hat{\theta}_i\}$

$a_0 = Enc_{\vec{x}_{I_0}}(m_0)$

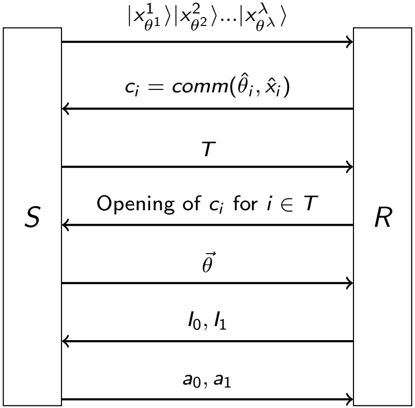
$a_1 = Enc_{\vec{x}_{I_1}}(m_0)$

$m_b = Dec_{\vec{\hat{x}}_{I_b}}(a_b)$

CK/BBCS protocol (II)

$\vec{x} \in \{0,1\}^\lambda$

$\vec{\theta} \in \{+,\times\}^\lambda$



$\vec{\hat{\theta}} \in \{+,\times\}^\lambda$

$\downarrow$Measurement

$\vec{\hat{x}} \in \{0,1\}^\lambda$

$I_b = \{i : \theta_i = \hat{\theta}_i\}$

$I_{\overline{b}} = \{i : \theta_i \neq \hat{\theta}_i\}$

$a_0 = Enc_{\vec{x}_{I_0}}(m_0)$

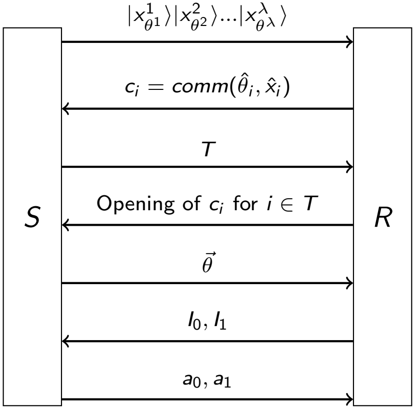
$a_1 = Enc_{\vec{x}_{I_1}}(m_0)$

$m_b = Dec_{\vec{\hat{x}}_{I_b}}(a_b)$

CK/BBCS protocol (II)

$\vec{x} \in \{0,1\}^\lambda$

$\vec{\theta} \in \{+,\times\}^\lambda$



$\vec{\hat{\theta}} \in \{+,\times\}^\lambda$

$\downarrow$ Measurement

$\vec{\hat{x}} \in \{0,1\}^\lambda$

$I_b = \{i : \theta_i = \hat{\theta}_i\} \setminus T$

$I_{\bar{b}} = \{i : \theta_i \neq \hat{\theta}_i\} \setminus T$

$a_0 = Enc_{\vec{x}_{I_0}}(m_0)$

$a_1 = Enc_{\vec{x}_{I_1}}(m_0)$

$m_b = Dec_{\vec{\hat{x}}_{I_b}}(a_b)$

Implemententing commitment scheme with simulation security from OWF

Implemententing commitment scheme with simulation security from OWF

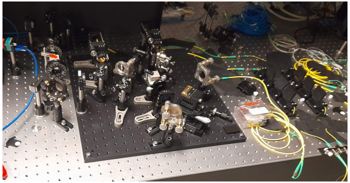
[BCKM21]	[GLSV21]
1. (Black-box) equivocality compiler	1. Equivocal commitment from Naor's commitment and zero-knowledge
2. Extractable commitment from equivocal commitment and quantum communication	2. Unbounded-simulator OT from equivocal commitment
	3. Extractable and equivocal commitment from unbounded-simulator OT and quantum communication

Features:

[BCKM21]	[GLSV21]
• **Black-Box** use of one-way functions	• **Constant-Round** OT in the CRS model
• **Statistical** security against malicious receiver	• **Statistically binding** extractable commitment

Further results

- QPKE from pseudo-random states (with special properties) [AQY'22]
- Practical protocols [D**G**ILYY'23 – on-going]
- Experimental implementation [IYYL**G**D'24 – on-going]



Weaker assumptions in the quantum world

Pseudo-random states

Pseudo-random states

Pseudo-random states $\{|\psi_k\rangle\}_k$

For every polynomial-time adversary $\mathcal{A}$, and polynomial ℓ:

$$|\Pr_k[\mathcal{A}(|\psi\rangle^{\otimes \ell}) = 1] - \Pr_{|\phi\rangle \sim \text{Haar}}[\mathcal{A}(|\phi\rangle^{\otimes \ell}) = 1]| \leq negl(n).$$

Pseudo-random states

Pseudo-random states $\{|\psi_k\rangle\}_k$

For every polynomial-time adversary $\mathcal{A}$, and polynomial ℓ:

$$|\Pr_k[\mathcal{A}(|\psi\rangle^{\otimes \ell}) = 1] - \Pr_{|\phi\rangle \sim \text{Haar}}[\mathcal{A}(|\phi\rangle^{\otimes \ell}) = 1]| \leq negl(n).$$

- PRS can be built from OWF [JLS'18]

Pseudo-random states

Pseudo-random states $\{|\psi_k\rangle\}_k$

For every polynomial-time adversary $\mathcal{A}$, and polynomial ℓ:

$$|\Pr_k[\mathcal{A}(|\psi\rangle^{\otimes \ell}) = 1] - \Pr_{|\phi\rangle \sim \text{Haar}}[\mathcal{A}(|\phi\rangle^{\otimes \ell}) = 1]| \leq negl(n).$$

- PRS can be built from OWF [JLS'18]
- Variants of PRS can be built from OWF [AGQY'22],[BBSS'23]

Pseudo-random states

Pseudo-random states $\{|\psi_k\rangle\}_k$

For every polynomial-time adversary $\mathcal{A}$, and polynomial ℓ:

$$|\Pr_k[\mathcal{A}(|\psi\rangle^{\otimes \ell}) = 1] - \Pr_{|\phi\rangle \sim \text{Haar}}[\mathcal{A}(|\phi\rangle^{\otimes \ell}) = 1]| \leq negl(n).$$

- PRS can be built from OWF [JLS'18]
- Variants of PRS can be built from OWF [AGQY'22],[BBSS'23]
- Constructions of strong primitives from PRS [AQY'22,...]

Pseudo-random states

Pseudo-random states $\{|\psi_k\rangle\}_k$

For every polynomial-time adversary $\mathcal{A}$, and polynomial ℓ:

$$|\Pr_k[\mathcal{A}(|\psi\rangle^{\otimes \ell}) = 1] - \Pr_{|\phi\rangle\sim\text{Haar}}[\mathcal{A}(|\phi\rangle^{\otimes \ell}) = 1]| \leq negl(n).$$

- PRS can be built from OWF [JLS'18]
- Variants of PRS can be built from OWF [AGQY'22],[BBSS'23]
- Constructions of strong primitives from PRS [AQY'22,...]
- Oracle separations between OWF and PRS [K'21,KQST'23]

Pseudo-random states

Pseudo-random states $\{|\psi_k\rangle\}_k$

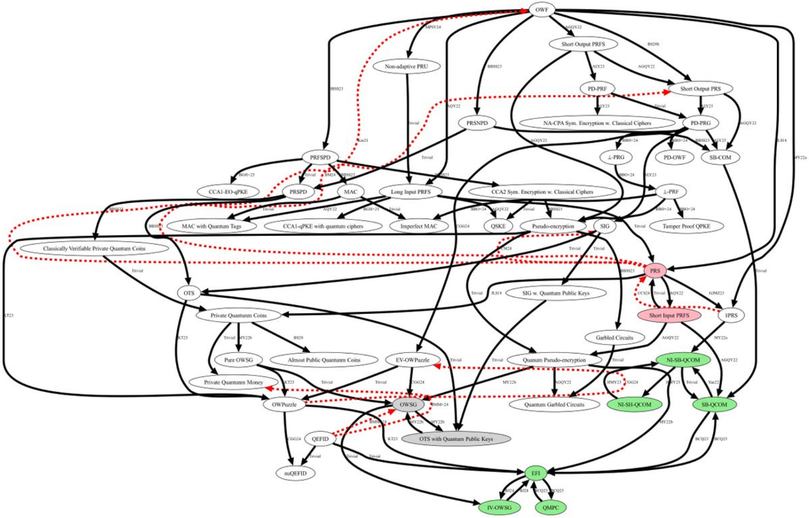
For every polynomial-time adversary $\mathcal{A}$, and polynomial ℓ:

$$|\Pr_k[\mathcal{A}(|\psi\rangle^{\otimes \ell}) = 1] - \Pr_{|\phi\rangle \sim \text{Haar}}[\mathcal{A}(|\phi\rangle^{\otimes \ell}) = 1]| \leq negl(n).$$

- PRS can be built from OWF [JLS'18]
- Variants of PRS can be built from OWF [AGQY'22],[BBSS'23]
- Constructions of strong primitives from PRS [AQY'22,...]
- Oracle separations between OWF and PRS [K'21,KQST'23]

OWF might not be the weakest computational assumption with quantum resources

Microcrypt? Nanocrypt?



Conclusions and open questions

Conclusions and open questions

- Quantum resources allow to implement classical primitives under weaker computational assumptions
  - PKE
  - MPC

Conclusions and open questions

- Quantum resources allow to implement classical primitives under weaker computational assumptions
  - PKE
  - MPC

- What is the minimal quantum computational assumption?
- More practical protocols?
- New impossibility results?

Conclusions and open questions

- Quantum resources allow to implement classical primitives under weaker computational assumptions
  - PKE
  - MPC
- What is the minimal quantum computational assumption?
- More practical protocols?
- New impossibility results?

Thank you for your attention!